

Intelligence-based Threat Assessments for Information Networks and Infrastructures

Author: Kent Anderson, CISM

Copyright © 2005 Network Risk Management, LLC. All rights reserved.

Information security is one of the hottest topics in the computer field. Awareness of its importance continues to grow with new reports of hackers, organized crime, fringe groups, and even terrorists exploiting technology for their own profit and motives. Many enterprises have suffered losses that can no longer be considered a cost of doing business. For example, the 2004 *E-Crime Watch Survey* published by CERT estimated that companies lost \$666 million from e-crimes in 2003. Recently, the Computer Security Institute and the Federal Bureau of Investigation reported in their 2005 Computer Crime and Security Survey that 56% of respondents experienced a security breach in 2004 and 13% didn't know if they had a security breach.

As businesses venture into electronic commerce, the need for secure networks is greater than ever before. Whole sectors of society such as banking and telecommunications are dependent on the availability of reliable and secure networks. Reflecting this fact is the ever-increasing size of the computer security marketplace (estimated by IDC to be \$45 billion in 2006) and the importance governments are beginning to place on protecting information infrastructures. Unfortunately, this increased investment does not appear to be mitigating the number or cost of incidents from either internal or external sources. There are several reasons for this. To name a few:

- Connectivity is increasing at a rate beyond the capacity to implement controls.
- Market pressures on hardware and software vendors reduce the introduction of security features and testing prior to product release.
- Retrofitting security into existing systems and applications is difficult, expensive, and, in some cases, impossible without serious operational impact.

However, a more fundamental problem exists in the implementation of controls:

Few organizations invest in proper risk assessment before implementing controls. Even fewer understand and qualify specific threats in order to evaluate risks accurately. The consequences can be profound. Not only are some threats overlooked, but also resources and budgets are misapplied to threats that do not exist or have minimal impact.

Fundamentally, security is the identification and management of risk.

At the same time, technology is changing faster than traditional risk assessment models can adapt. Organizations are not simply increasing the size of their networks by adding more systems; they are also adding new dimensions of connectivity and complexity. Back-end business processes such as suppliers, contractors, and partners and front-end processes such as clients and customers are increasingly integrated into a seamless network. To make matters worse, the inherently insecure Internet and underlying telecommunications infrastructure are the de facto standard means of providing connections.

These multidimensional information architectures create *information infrastructures* that cross both organizational and national boundaries where no single entity, governmental or private, has control or responsibility for security. One example of an information infrastructure is the Internet itself. Other information infrastructures can be defined in terms of the information component of traditional social infrastructures. These include telecommunications, healthcare, finance, government and defense, oil & gas, power generation, transportation, and water management.

This paper will discuss threat assessments, risk assessments, and information infrastructures in general and provide an overview of an *intelligence-base* threat assessment model developed by Network Risk Management, LLC. This model scales from a single organization to information infrastructures. Proper and accurate threat assessments will allow computer security experts, vendors, and government agencies to better predict future vulnerabilities and mitigate damages.

Threats and Risks

Risk is generally defined as “the possibility of loss”. As it applies to information technology, risk is “the possibility for loss of availability, integrity, or confidentiality due to a specific threat”.

Risk assessment is the analysis of the likelihood of loss due to a particular *threat* against a specific *asset* in relation to any *safeguards* to determine *vulnerabilities*. Assets are those objects, both physical (buildings, computer hardware, laptops) and virtual (e-mail, software, databases) having value to an organization. **Error! Reference source not found.** shows the process of evaluating risk.

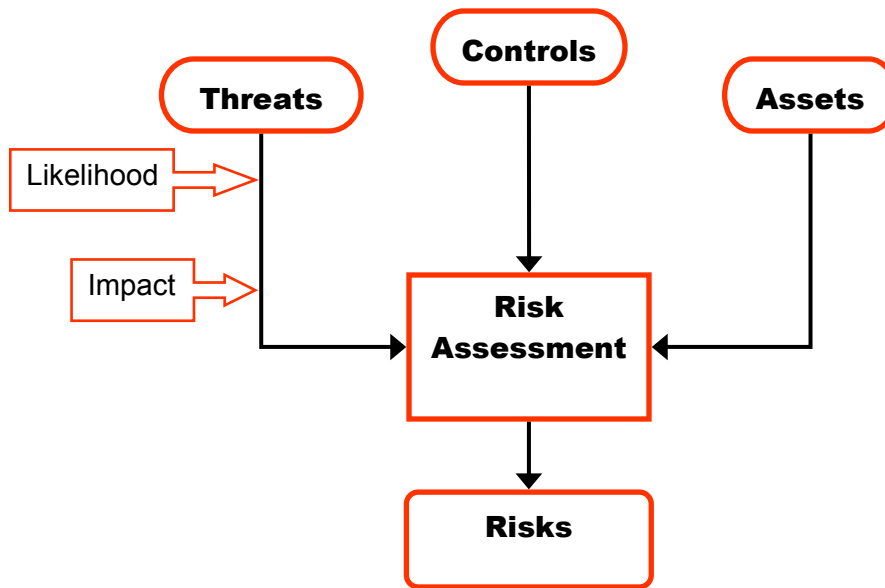


Figure 1 - Qualitative Risk Assessment Process

The effectiveness of any risk assessment process relies on the accuracy and completeness of the inputs. Unfortunately, almost all risks assessments methods used today do not provide a method to assess accurately the threats facing a large networked environment. Identification and evaluation of threats is a complicated, multi-dimensional process. This process involves the analysis of multiple technologies and how they inter-operate. It involves the analysis of methods, access, skill levels, and costs required to exploit a given weakness. Threats to information assets are not limited to technological weaknesses. Physical controls, business and operational processes, telecommunications, and employee awareness all play vital roles. Not all threats are malicious. Accidents, errors of omission, and natural disasters are equally likely threats requiring consideration.

Risk assessments only provide a snapshot of vulnerabilities in an ever changing, dynamic system. In large networks, there are continuous changes in the number and type of systems, connections, and software. Information and physical assets, potential safeguards, and business requirements also always evolving. Therefore, risk assessments must be part of an ongoing process re-evaluating old vulnerabilities and identifying new ones. Only after actual threats and vulnerabilities are understood can policy and risk management decisions be implemented.

Because of the complexity and effort involved in analyzing these multi-dimensional factors, a separate *threat assessment* is required. Traditionally, threat assessments attempt to determine what threats exist, their likelihood, and the consequences or potential loss [1 1994]. Later, this paper will present an expanded definition and process of threat assessment to address these complexities in very large information networks and infrastructures.

Information Systems, Networks and Infrastructures

Before discussing a new model for threat assessment, it is important to understand information architectures and how they scale from individual systems to infrastructures.

The basic building block in any network is the individual computer. Figure 2 shows a simplified view of the components that make up a single system. For the most part, the theoretical security model at this level is well-understood [2 1988]. A single system usually is under the control of a single owner and is located in a specific physical location.

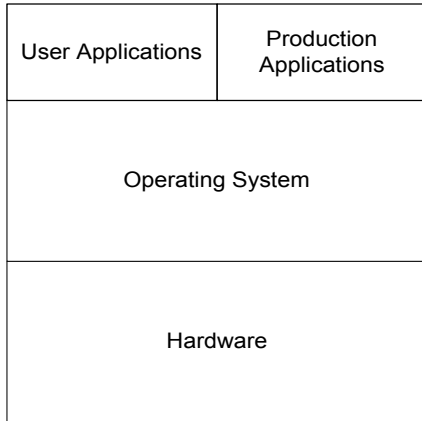


Figure 2- Simplified system components

With the addition of communication protocols (software) and channels (hardware), individual systems can be connected to create a network of systems. The size of a network can range from two systems to the limits of the protocols and channels (usually millions of systems). Using simple industry standard protocols (TCP/IP, etc.), an almost infinite number of different networks can be created. Individual systems are placed in different physical locations, manufactured by different vendors, and owned by different

organizations.

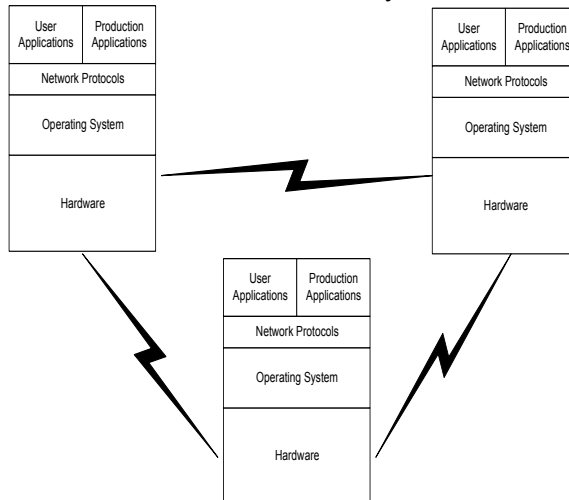


Figure 3 shows the components of a simple network.

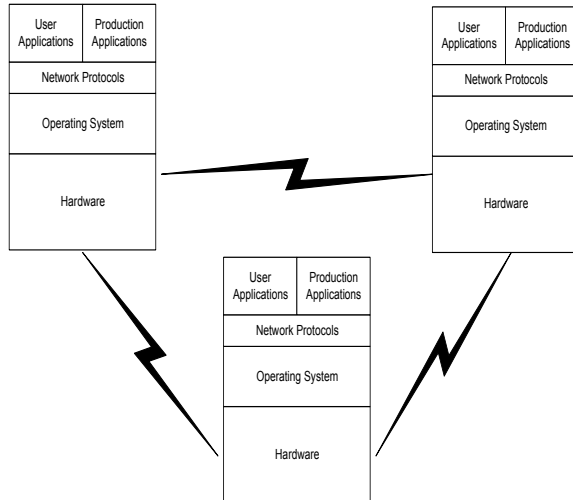


Figure 3- Simplified network of three systems

It is important to realize that networks are designed to have temporal flexibility as well: Individual systems can be added or removed from the network at any time. Therefore, large networks are very dynamic in their structure and operation.

Systems within a network may perform multiple functions. For example, a single system may act as a network router, provide interactive word processing to users, and store and analyze sales data. Because of this virtual nature, networks are often drawn as clouds in schematic diagrams.

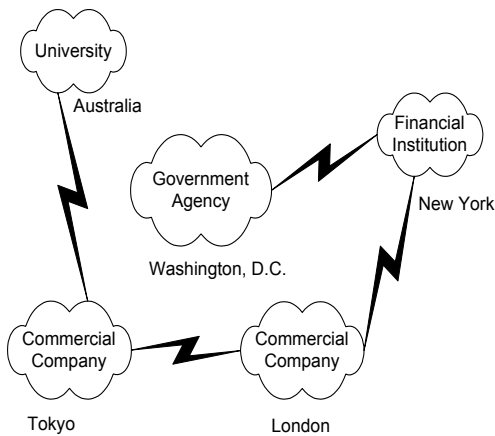


Figure 4 - Simplified internet example

To add further complexity, individual networks can be joined together to form larger networks called internets as shown in Figure 4. When discussing internets, it is sometimes helpful to view the network as a single entity. Again, the size of these internets can scale from two networks upward. The number of permutations in these super networks is, for all practical purposes, infinite. There are few physical limitations on these networks and they often cross-organizational and national boundaries.

Finally, the concept of infrastructure is introduced. Infrastructures are defined as *the basic structural foundations of a society*. Several infrastructures are considered critical to society, commerce, and national security: Telecommunications, the Internet, transportation, emergency services, oil & gas, power generation & distribution, healthcare and finance. Each of these infrastructures has an information component that uses and is reliant on computers and networks to provide services.

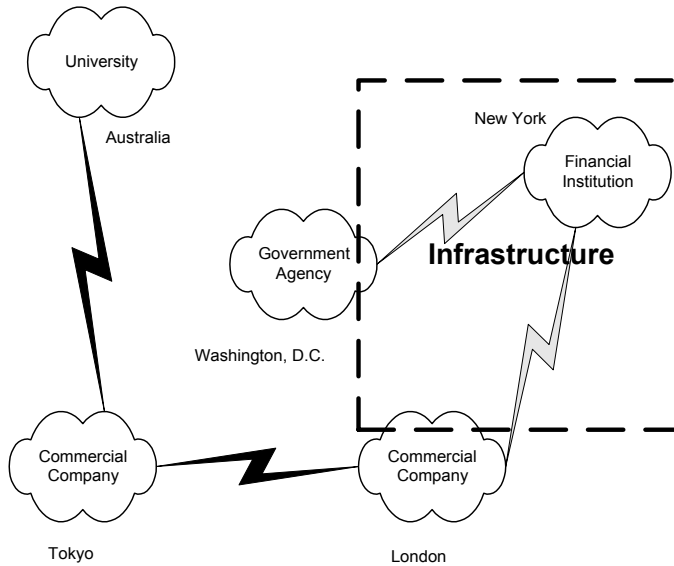


Figure 5 - Simplified diagram of relationship between inter-networks and infrastructures

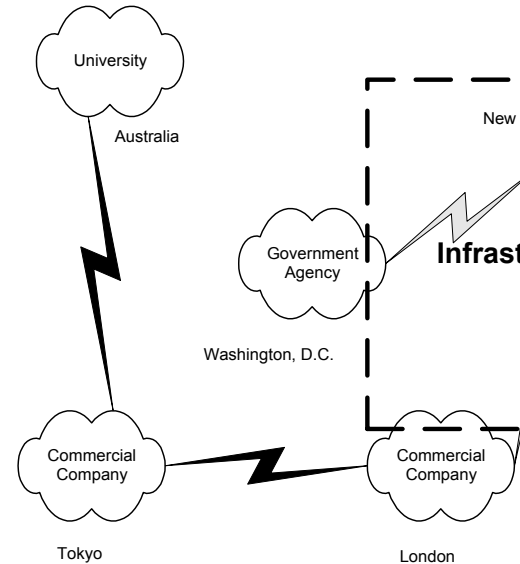


Figure 5 shows a conceptual diagram relating an information infrastructure to an internet.

The information component of this infrastructure encompasses many systems connected in different networks owned by government agencies, commercial organizations, and financial institutions. Furthermore, because of the highly connected nature of internets, unrelated networks and systems have potential access to the systems within the infrastructure.

A complete analysis of information infrastructures is beyond the scope of this paper, but several attributes have significant impacts on security. First, these infrastructures are highly inter-dependent. For example, the Internet requires telecommunications and power generation. Power generation is dependent on oil & gas and so on.

Because of the size, complexity, physical and organizational distribution, and rate of change in the underlying networks, it is impractical to ever fully diagram or map out the information component of an infrastructure. It is these attributes of information infrastructures that create security vulnerabilities and precludes the implementation of strong security measures.

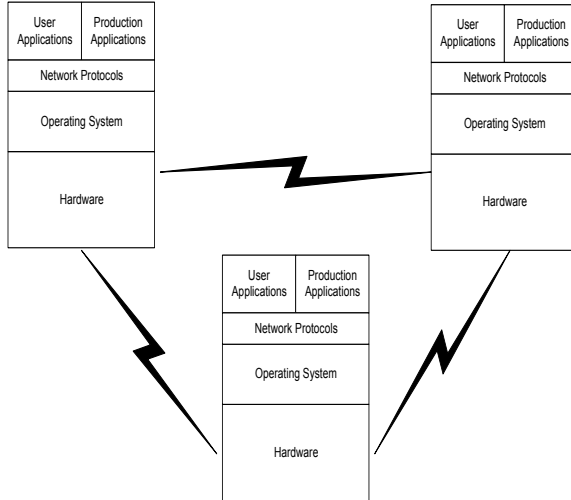


Figure 2 and

Figure 3 presented the simplified hardware and software components in an information system. Large networks and information infrastructures can be diagrammed to show

User Applications (Word Processing, E-mail, etc.)	Other Production Applications
Infrastructure Applications such as telecommunication switching and billing	
Network Protocols (TCP/IP, etc.)	
Operating Systems (NT, Unix, MVS, VMS, etc.)	
Hardware (Processors, Communication Channels, Storage Devices, etc.)	

underlying logical components as in

Figure 6. In this diagram, each component represents the logical aggregation of what physically may represent thousands of different systems and applications.

User Applications (Word Processing, E-mail, etc.)	Other Production Applications
Infrastructure Applications such as telecommunication switching and billing	
Network Protocols (TCP/IP, etc.)	
Operating Systems (NT, Unix, MVS, VMS, etc.)	
Hardware (Processors, Communication Channels, Storage Devices, etc.)	

Figure 6 - Simplified diagram of the components of a hypothetical telecommunications infrastructure

A critical, and often overlooked, aspect of security can be stated as follows:

Vulnerability at a lower functional level of a system (or network) undermines safeguards at higher levels.

For example, password controls employed at the application level can be undermined within the network protocol, operating system, or hardware levels as demonstrated by packet sniffers employed in password grabbing. Likewise, encryption schemes implemented in the network protocols can be attacked at the hardware or operating system level. This is particularly important when discussing security in widely distributed networks and infrastructures since vulnerabilities in a component of a single computer system may expose information or controls in other computer systems.

Implications to Security

Information security experts have traditionally studied threats on the scale of individual computers or organizational networks. While this is a valid practical approach, it does not reflect the reality of actual or potential threats such as those described above. When computer misuse is evaluated from the view of the intruder, artificial boundaries such as

organizational ownership or national borders are meaningless.

A critical challenge to security experts, law enforcement, and intelligence agencies is the ability to identify emerging new threats. This has been especially difficult in the arena of information security for several reasons:

- Law enforcement and information security experts for the most part do not use an intelligence-driven approach for prevention and control of computer crime. Investigations tend to be reactive and event-driven. While this has limited effectiveness for simple system intrusions, it will not be adequate for sophisticated or infrastructure attacks. Unless a more analysis-based process is employed, prevention will continue to lag behind the threat curve.
- The speed at which new technology is introduced creates a rapidly moving target for threat assessments. Each new technology requires high level technical expertise to analyze. By the time vulnerabilities are identified technology has changed again.
- Key governmental and industry policy makers lack a understanding of technology or the multi-dimensional aspects of information security. Many security professionals are biased toward a particular product such as intrusion detection systems or firewalls that limit the scope of proposed solutions.

- Exaggeration of threats and capabilities by some security consultants and the press and the sympathetic portrayal of low-level intruders by others have caused a counter-reaction dismissing potential threats.
- Confidentiality, fear of publicity, and inaccurate or incomplete open source information makes complete analysis difficult.

Perfectly accurate prediction of exactly when, how, and by whom a potential threat will manifest itself is impossible. However, intelligence-driven analysis can detect specific enabling activity and other indicators that allow prediction of new threats. This information can be used in traditional risk assessments to better choose controls and provide justification for budget and resource decisions.

Infrastructure and System Attacks

Historically, information security threats have targeted individual systems. The motive for these attacks varied, but the methods and goals were limited to the computer system as the primary target. A fundamental change is occurring in information security: Automation and globalization combined with increased criminal attention are exposing whole infrastructures to targeted attack.

Attacks against infrastructure are relatively new and are of interest in the study of information warfare. In considering infrastructure vulnerabilities, threats to both individual systems and the infrastructure itself must be evaluated when considering criminal activity. Both share similar enablers as a pre-requisite to compromise, however, infrastructure attacks require a more concerted and coordinated effort and provide better data points for indicator and warning analysis. It is important to distinguish between the two types of attacks in threat assessments. Therefore, the following definitions are offered:

Infrastructure Attack (IA) - An attack designed to compromise significantly the function of a whole infrastructure rather than individual components.

Systems Attack - An attack targeted against individual systems or control centers which is not detrimental to the overall operation of a whole infrastructure or organization.

Further, it is important to assess the potential and actual damage from these attacks. To begin this process, we define:

Successful System Attack - An intrusion where the basic integrity of a system is compromised. This compromise may lead to the loss of confidentiality, data integrity, or system resource availability. However, the attack does not target the infrastructure in which the computer operates.

Successful Infrastructure Attack - An IA capable of sustaining compromise beyond a temporary period. This will usually require attacking recovery systems as well. A successful IA may lead to cascading failure into other infrastructures. The longer the compromise is sustained, the further the effects will propagate. A successful attack would most likely be viewed as a national security threat by most countries.

Limited Infrastructure Attack - An attack against an infrastructure that causes significant damage and cost, but is recovered without major disruption and does not affect other infrastructure components i.e. disruption is localized and contained. A limited infrastructure attack would mimic a major natural disaster such as a power outage experienced by a heavy snowstorm.

Successful attacks against information infrastructures are possible though very difficult to carry out. The only known attempted attack against an infrastructure (the

telecommunications infrastructure) was initiated by the Chaos Computer Club (CCC) in Germany in September 1995. The CCC called for a denial of service attack against French telecommunications systems to protest nuclear testing in the Pacific [3 1995]. This attack had no impact.

Currently, there is significant debate within the security community concerning the ease with which successful attacks can be carried out. If a successful attack were simple, malicious code such as computer viruses or normal component failure would have already caused massive damage. Successful infrastructure attacks will require precise targeting and successful, coordinated attacks against multiple system and control points with exact timing to compromise system redundancy. Attacks may also require compromising multiple levels in the infrastructure architecture (i.e. applications, protocols, system software, and hardware) as well as recovery systems such as backup operations. With this said, the ability to cause damage that once required the military of a nation-state is now within reach of much smaller, less organized groups.

Threat Assessments: Enablers and Indicators

As discussed in the last section, the success of an attack depends on more than the exploitation of a single vulnerability. Multiple enabling events, as well as significant planning and technical knowledge (both at the system and application level), are required. Because of this, an expanded form of threat assessment is required not only to identify potential threats, but also to understand their likelihood of occurring.

Isolated attacks or accidents can be very costly to an organization. However, the potential damage and impact of a limited or successful infrastructure attack dwarf these costs. At this level, losses can be considered issues of national security. Therefore, while the emphasis on implementing safeguards within these networks and systems must be improved, security experts, law enforcement, and national intelligence agencies must place a greater emphasis on detecting and preventing these types of attacks.

With this in mind, Network Risk Management, LLC has developed an expanded threat assessment method. The goals of this new model are twofold:

- 1) Identify threats based on feasibility (enablers) and indicators of potential exploitation. These threats are further categorized by the potential likelihood they will be exploited.
- 2) Provide an intelligence-based method of predicting, detecting, and monitoring potential large-scale threats to business and national security.

This model will scale from small networks to large internets and infrastructures. Figure 7 shows the components and processes in this threat assessment.

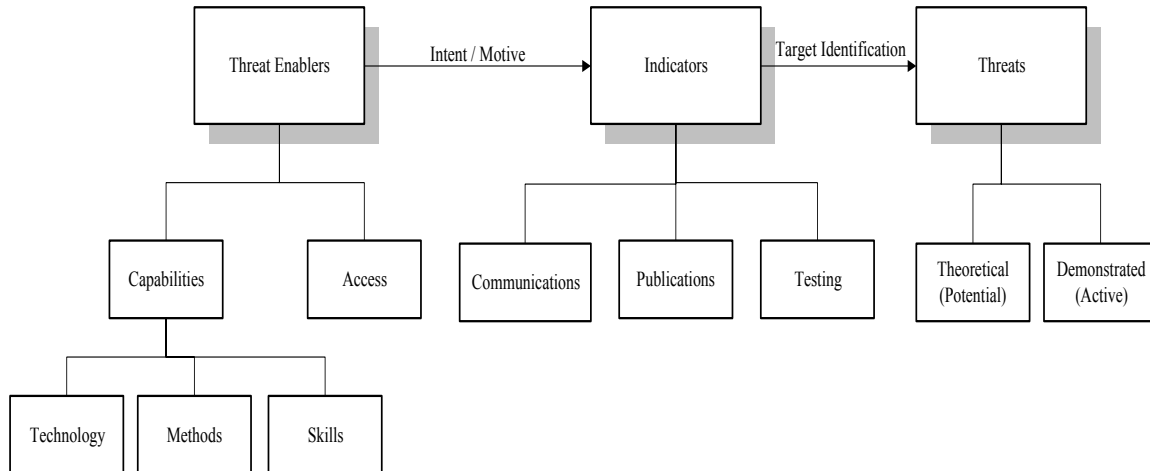


Figure 7 - Information threat assessment model

Threat Enablers

Two elements are required for a threat to exist: First, there must be the *capability* for a threat to occur. Secondly, it must be possible to exploit the capability. In terms of information security, this requires *access*, either logical or physical. When both of these elements exist, they create a *threat enabler*.

The capability for a threat to exist may be based on many factors. Figure 7 shows three such factors: Technology, Methods, and Skills. The movement to mobile and wireless networks is an example of technologies that enable new threat capabilities.

Methods are the techniques used to create or exploit a threat. Examples may vary from social engineering to password guessing algorithms. Finally, skills are required to exploit the threat. This includes general technical, application and business process knowledge. Some threats require minimal skills others require extensive expertise to exploit successfully. Understanding the methods available and the skill level required are important considerations in determining threat capabilities.

Identifying threat enablers is a first but insufficient step in the threat assessment process. Proper application on this process yields a staggering number of potential threats. Many will never be exploited; others require significant investment by the attacker. Therefore, further analysis is required to refine the likelihood of a threat actually occurring. This is critical since resources to mitigate or prevent threats are limited and should be applied where they will be most effective.

Threat Indicators

In this threat assessment model, enablers are further prioritized using an intelligence-based process to detect the presence of specific *indicators* of potential activity. A prerequisite of indicators is intent or motive. The importance of this requirement as it applies to infrastructure attacks and information warfare was summed up by CIA Director Deutch in his June 25, 1996 testimony before the U.S. Senate. Intent and motive also help to qualify the potential effort, skill, and the expense an attacker is willing to invest in exploiting a vulnerability.

Indicators are specific actions on the part of individuals, groups, or organizations. An example of open-source indicators would be the communication of specific threat enablers in Usenet news groups or presented at a security conference. The method used to exploit vulnerabilities could be published on a web site. Another example would be testing methods of exploiting vulnerabilities or simply demonstrating the feasibility of the threat. If indicators are present, they create a greater potential that the enablers will be exploited and more effort should be placed into safeguards or investigation of activity.

The final prioritization of threats takes place when there are indications of targeting against a specific information asset. When this occurs, threats can be categorized as either *potential* (i.e. the attack has not actually taken place) or *active* (an attack has been attempted or in some other way demonstrated to be feasible). In considering implementation of security controls, these threats, if applicable to the information assets of an organization, should receive the highest effort and priority.

Conclusions and Recommendations

As society becomes more dependent on information processing and communication, the potential for significant loss increases if these systems are disrupted. With the ever-increasing complexity of technological change and connectivity, new threats are continuously appearing and when considering risks to information infrastructures, the number, type, and variation of threats are overwhelming.

This paper has presented a new model of threat assessment created by [Network Risk Management, LLC](#). This model is designed to help identify potential threats in a more structured manner. Furthermore, these threats are prioritize based on specific information about the effort required to exploit them and indicators of the likelihood they will be exploited.

The application of this model requires a new way of thinking about threat assessment. First, threat assessments must be recognized as a distinct and ongoing process. Secondly, it requires a continuous data gathering and analysis (intelligence) process to identify new and changing threats effectively.

Security managers and experts can use this model to better employ traditional risk assessment methods as well as develop and implement better controls. Additionally, this model can provide law enforcement and government agencies with a valuable tool in evaluating where scarce resources should be applied in monitoring criminal and national security threats in the information age.

References

- Communications Security Establishment, "Threat and Risk Assessment Working Guide", October, 1999.
- Gasser, M.A., "Building a Secure Computer System", Van Nostrand Reinhold, New York, 1988.
- Chaos Computer Club, "Stop the Test", <http://www.zerberus.de/texte/aktion/atom/>, September 1, 1995.

OTHER PAPERS BY KENT ANDERSON, CISM

["Convergence: A Holistic Approach to Risk Management"](#) published in *Network Security*, Elsevier Ltd., Volume 2007, Issue 5, May, 2007.

Frustration grows as security practitioners feel more pressure and accountability to perform – yet never seem to have the resources to get the job done. "Executives just don't get it" is probably the most common explanation but have we ever stopped to ask if maybe we don't get it?

Every year IT security managers develop new budgets requesting more funds and resources to stem the tide of endless security issues – patching, virus management, provisioning, installation of new appliances, the list goes on. Every year business leaders listen to these requests and usually provide a fraction of the requested increases. This cycle has become a ritual in the IT security profession and fits Albert Einstein's definition of insanity: Doing the same thing over and over again expecting different results.

["IT Security Professionals Must Evolve for Changing Market"](#) published in SC Magazine, October 12, 2006.

IT security awareness is at an all-time high, and organizations are spending and hiring in record numbers. Legislation and regulations are proliferating. Yet, for all this effort, nearly every statistical measure of IT security performance – from the number of incidents and vulnerabilities to the cost and impact of a security breach – is bad news. In what other endeavor would so much investment be permitted with such poor results?

The potential for disruption from malicious or accidental threats is growing, yet our ability to manage risk has never been more uncertain. Throwing more money at IT security will not close the gap.

["Managing the Cyber Threat"](#)

Technology is not the only source of risk to information infrastructures. Political, physical, environmental, legal and regulatory issues are all factors contributing to the creation of a multi-dimensional problem. While prevention is the preferred course of action, no security measures are perfect. Organizations must be prepared to quickly detect and effectively respond to the threats they face in the ever-changing e-business environment.

["Intelligence-Based Threat Assessments"](#)

Few organizations invest in proper risk assessment before implementing controls. Even fewer have the capability to understand and qualify specific threats to their information assets in order to assess risks accurately. The consequences can be profound. Not only are some threats overlooked leaving inadequate controls, but also scarce resources and budgets may be misapplied to threats that do not exist or have minimal impact. This paper will discuss threat assessments, risk assessments and information infrastructures in general and provide an overview of an intelligence-base threat assessment model.

["Criminal Threats to Business on the Internet: A White Paper"](#)

This paper looks at the increasing trend of criminal activity against information systems, from the low-level, amateur intruder to organized crime, industrial and international espionage. In addition, the author looks how this activity is likely to evolve in the near future.

["International Intrusions: Patterns and Motives"](#)

Summary of the author's investigation of international intrusions presenting a classification model of attributes and motives displayed by intruders and explaining common patterns of activities. The author argues that common methods of investigating computer intrusions are limited in scope, therefore, security solutions and tools have limited effectiveness.

ABOUT NETWORK RISK MANAGEMENT, LLC

Network Risk Management, LLC (NRM) provides clients with **informed risk management strategies™**. Informed decision making not only reduces loss and exposure to potential risks, it allows executives to make effective investment decisions concerning risk management. NRM provides solutions to two broad clientele – enterprise and security providers.

Enterprise risk management is a complex matter, involving more than technical considerations – it involves people, policy, process and technology. In order to meet these requirements, NRM developed an **ENHANCED SECURITY ASSESSMENT FRAMEWORK (ESAF)™** methodology.

The **ESAF™** methodology to assist enterprise clients streamline their security organization and operations using four guiding principles:

1. **Alignment** of security with business objectives to enable and support the organization;
2. **Convergence** of security strategies to maximize return on investment – traditional models of separate security functions are wasteful and hinder management of cross-functional risk;
3. **Risk-based** decision making founded on understanding the unique threats and risks to each organization; and,
4. **Strategic** focus to transform the security organization from tactical and fire-fighting to strategic and pro-active.

Services include (for both physical and IT security):

- Threat and risk assessments
- Standard security reviews
- Strategic security architecture analysis
- Incident response evaluation and planning
- Policy review and development
- Executive awareness presentations and briefings
- Training programs for security personnel

NRM also assists *security providers* in creating competitive offerings through development of security service portfolios, reference architectures, differentiated capabilities, competitive assessment, go-to market strategies and other support services.

ABOUT KENT ANDERSON, CISM

Mr. Anderson is considered a leading authority on security, with more than 21 years of experience in the field. He is the founder and Managing Director of Network Risk Management, LLC (NRM) located in Portland, Oregon.

Mr. Anderson's international experience includes risk and threat assessment, designing and managing security organizations and operations, investigations and developing security businesses.

Mr. Anderson's expertise is founded in understanding the real-world threats. He has led or coordinated numerous international investigations including espionage, industrial espionage, computer misuse (hacking), sexual harassment, threats of violence, extortion, fraud, intellectual property thefts, copyright infringement and product counterfeiting. These investigations have resulted in the successful prosecution of 10 individuals and numerous successful civil cases.

Mr. Anderson has been quoted by numerous publications including the Washington Post, CNN, Associated Press, Reuters, USA Today, Los Angeles Business Daily, Singapore Business Times, Danish National Radio (DR) and the BBC.

He has provided training and assistance to various law enforcement and government agencies including the FBI, U.S. Secret Service, Department of Defense, Department of Justice, FLETC, Scotland Yard, the German BKA, the Russian MVD and Norwegian, Danish and Swiss police. Additionally, he provided consulting to the Organization for Economic Cooperation and Development (OECD) on international harmonization of computer crime laws and the British Houses of Parliament on the development of the U.K.'s Computer Misuse Act.

He has held positions as Senior Vice President of IT Security and Investigations with an international business risk consultancy, as Director in the Dispute Analysis & Investigations group of PricewaterhouseCoopers, LLP and as the European Information Security Manager for Digital Equipment Corporation.

Mr. Anderson is a Certified Information Security Manager and serves on Motorola's Research Visionary Board and on ISACA's Security Management Advisory Committee.

Contact Network Risk Management, LLC to find out how your organization can implement *informed risk management strategies™*:

Kent Anderson, CISM

Managing Director

NETWORK RISK MANAGEMENT, LLC

Portland, OR USA

+1 (503) 203-8295